# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-146843
(43)Date of publication of application : 06.06.1997

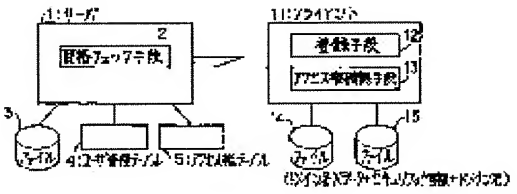
(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 07-301029
(22)Date of filing : 20.11.1995

(71)Applicant : FUJITSU LTD
(72)Inventor : YAMAMOTO MASAHIKO

## (54) INFORMATION PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To easily manage the security of a stored file by reading security information from the file for storing the security information for which access is requested at the time of access request, collating inputted information with read information and accessing the file when it is judged that an access right is present.
SOLUTION: A registration means 12 registers data, a domain name and the security information in the file and registers a prescribed domain name to a device, etc. An access right confirmation means 13 confirms the access right based on the domain name and the security information stored in the file. At the time of the access request, the access right confirmation means 13 reads the security information from the tile for which the access is requested and collates the inputted information with the read security information, and when it is judged that the access right is present, the tile is accessed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平9－146843
(43)公開日　平成９年(1997)６月６日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | | 技術表示箇所 |
|---|---|---|---|---|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３１０ | | Ｇ０６Ｆ | 12/14 | ３１０Ｋ | |
| | 12/00 | ５３７ | | | 12/00 | ５３７Ａ | |

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）

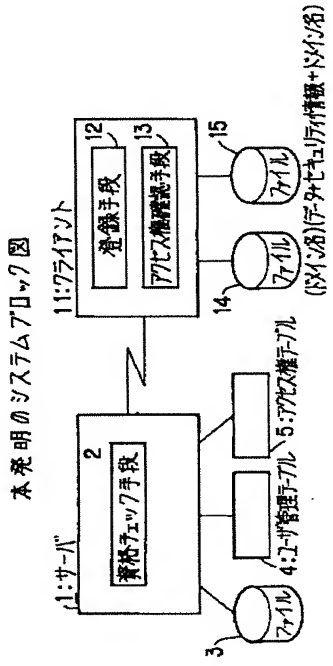
(21)出願番号　特願平7－301029

(22)出願日　平成７年(1995)11月20日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　山本　雅彦
静岡県静岡市伝馬町16番地の３　株式会社富士通静岡エンジニアリング内
(74)代理人　弁理士　岡田　守弘

(54)【発明の名称】　情報処理装置

(57)【要約】
【課題】　本発明は、ファイルのセキュリティを行う情報処理装置に関し、セキュリティ機構を持たない情報処理装置であってもファイル毎に所有者ＩＤ、グループ名、グループの権限の有無などのセキュリティ情報およびドメイン名を書き込んでおき、これらをもとにアクセス権の有無をチェックしてセキュリティを管理することを目的とする。
【解決手段】　データを受信あるいはデータを作成したときに当該データを格納すると共に、セキュリティ情報を格納するファイルと、アクセス要求時に、アクセス要求のあったファイルからセキュリティ情報を読み出し、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときに当該ファイルのアクセスを行う手段を備えるように構成する。



1

【特許請求の範囲】
【請求項１】ファイルのセキュリティを行う情報処理装置において、
データを受信あるいはデータを作成したときに当該データを格納すると共に、セキュリティ情報を格納するファイルと、
アクセス要求時に、アクセス要求のあった上記ファイルからセキュリティ情報を読み出し、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときに当該ファイルのアクセスを行う手段を備えたことを特徴とする情報処理装置。
【請求項２】ファイルのセキュリティを行う情報処理装置において、
データを受信あるいはデータを作成したときに当該データを格納すると共に、ドメイン名を格納するファイルと、
アクセス要求時に、アクセス要求のあった上記ファイルからドメイン名を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致してアクセス権有と判明したときに当該ファイルのアクセスを行う手段を備えたことを特徴とする情報処理装置。
【請求項３】ファイルのセキュリティを行う情報処理装置において、
データを受信あるいはデータを作成したときに当該データを格納すると共に、ドメイン名およびセキュリティ情報を格納するファイルと、
アクセス要求時に、アクセス要求のあった上記ファイルからドメイン名およびセキュリティ情報を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致したときに、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときに当該ファイルのアクセスを行う手段を備えたことを特徴とする情報処理装置。
【請求項４】上記アクセス要求時に、アクセス要求のあった上記ファイルからセキュリティ情報を読み出し、入力されたユーザＩＤが読み出した所有者ＩＤに一致したとき、入力されたグループ名が読み出したグループ名に一致しかつ読み出したグループに対するアクセス権が有のとき、あるいは入力されたグループ名が読み出したグループ名に一致しなくかつ読み出したグループ以外に対するアクセス権が有のときに、当該ファイルのアクセスを行う手段とを備えたことを特徴とする請求項１あるいは請求項３記載の情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ファイルのセキュリティを行う情報処理装置に関するものである。
【０００２】
【従来の技術】従来、セキュリティ機構を持たないクライアント（情報処理装置）では、ディスク装置に記憶されたファイルや、ＦＤ（フロッピィディスク媒体）やＭＯ（光磁気ディスク媒体）などに記憶されたファイル毎にパスワードを書き込み、ファイルのアクセス要求するときにパスワードを入力して一致したときにのみアクセス許可してセキュリティを確保するようにしていた。

2

【０００３】
【発明が解決しようとする課題】上述したセキュリティ機構を持たないクライアントでは、ファイル毎にパスワードを書き込んでおき、アクセス要求時に入力されたパスワードと一致したときにファイルアクセスを許可するようにしていたため、パスワードの設定、アクセス時のパスワード確認、パスワードの変更などに利用者にとって大きな負担となってしまう問題があった。また、ファイル毎にパスワードを書き込んでいたため、個人のファイルのセキュリティの管理に限られてしまい、会社組織の部単位、課単位にアクセス権の有無などのセキュリティ管理を行い難いという問題があった。
【０００４】本発明は、これら問題を解決するため、セキュリティ機構を持たない情報処理装置であってもファイル毎に所有者ＩＤ、グループ名、グループの権限の有無などのセキュリティ情報およびドメイン名を書き込んでおき、これらをもとにアクセス権の有無をチェックしてセキュリティを管理することを目的としている。
【０００５】
【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、登録手段１２は、データ、ドメイン名、およびセキュリティ情報をファイルに登録したり、所定のドメイン名を装置に登録したりなどするものである。
【０００６】アクセス権確認手段１３は、ファイルに格納されているドメイン名およびセキュリティ情報をもとにアクセス権を確認するものである。次に、動作を説明する。
【０００７】アクセス要求時に、アクセス権確認手段１３がアクセス要求のあったファイルからセキュリティ情報を読み出し、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときにファイルのアクセスを行うようにしている。
【０００８】また、アクセス要求時に、アクセス権確認手段１３がアクセス要求のあったファイルからドメイン名を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致してアクセス権有と判明したときにファイルのアクセスを行うようにしている。
【０００９】また、アクセス要求時に、アクセス権確認手段１３がアクセス要求のあったファイルからドメイン名およびセキュリティ情報を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致したときに、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときにファイルのアクセスを行うようにしている。

【００１０】また、アクセス要求時に、アクセス権確認手段１３がアクセス要求のあったファイルからセキュリティ情報を読み出し、入力されたユーザＩＤが読み出した所有者ＩＤに一致したとき、入力されたグループ名が読み出したグループ名に一致しかつ読み出したグループに対するアクセス権が有のとき、あるいは入力されたグループ名が読み出したグループ名に一致しなくかつ読み出したグループ以外に対するアクセス権が有のときに、ファイルのアクセスを行うようにしている。

【００１１】従って、セキュリティ機構を持たない情報処理装置であっても、ファイル毎に所有者ＩＤ、グループ名、グループの権限の有無などのセキュリティ情報およびドメイン名を書き込んでおき、アクセス権確認手段１３がこれらをもとにアクセス権の有無をチェックしてセキュリティを管理することが可能となる。

【００１２】

【発明の実施の形態】次に、図１から図８を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１３】図１は、本発明のシステムブロック図を示す。図１において、サーバ１は、回線を介して１つあるいは複数のクライアント１１と接続しファイルの一括管理するものであって、ここでは、資格チェック手段２などから構成されるものである。

【００１４】資格チェック手段２は、クライアント１１から回線を介して接続されたときに、ユーザの資格をチェックするものであって、例えばユーザＩＤ、パスワードなどでその資格をチェックするものである。

【００１５】ファイル３は、管理するデータを格納するものである。ユーザ管理テーブル４は、ユーザを管理するものであって、例えばユーザＩＤに対応づけてパスワードおよび属するグループ名（例えば総務課）などを予め登録するものである（図２参照）。

【００１６】アクセス権テーブル５は、ユーザのアクセス権を管理するものであって、例えばディレクトリあるいはそのファイル毎に所有者、グループ、その他などの情報を登録するものである（図３参照）。

【００１７】クライアント１１は、サーバ１に回線を介して接続して各種業務処理を行うものであって、ここでは、登録手段１２、およびアクセス権確認手段１３などから構成されるものである。

【００１８】登録手段１２は、データ、ドメイン名、およびセキュリティ情報をファイルに登録したり、ドメイン名を装置に登録したりなどするものである（図４ないし図７を用いて後述する）。

【００１９】アクセス権確認手段１３は、ファイルに格納されているドメイン名およびセキュリティ情報をもとにアクセス権を確認するものである（図６ないし図８を用いて後述する）。

【００２０】ファイル１４は、クライアント１１という装置に対応づけてドメイン名を登録するものである。ファイル１５は、データにセキュリティ情報（所有者ＩＤ、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）およびドメイン名などを登録するものである。

【００２１】図２は、本発明のユーザ管理テーブル例を示す。このユーザ管理テーブル４は、図示のように、ユーザＩＤに対応づけて下記の項目を予め登録したものである。

【００２２】

**・ユーザＩＤ：Ｕ０１**
**・パスワード：０１１**
**・グループ名：Ｘ**
**・その他**

ここで、ユーザＩＤは、クライアント１１あるいはその利用者に対して一意に割り当てられたＩＤである。グループ名は、利用者の属するグループ名である。

【００２３】以上のように、ユーザＩＤに対応づけてパスワードおよびグループ名などを予めユーザ管理テーブル４に登録しておくことにより、クライアント１１から回線を介してサーバ１に接続し、サーバ１のファイル３からデータをダウンロードしようとするときに、資格チェック手段２が資格をチェックしてＯＫのときにファイルおよびセキュリティ情報（所有者ＩＤ、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）をダウンロードすることが可能となる。

【００２４】図３は、本発明のアクセス権テーブル例を示す。このアクセス権テーブル５は、サーバ１がセキュリティ管理するファイル３について、ディレクトリ毎にセキュリティ情報（所有者ＩＤ、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）および各ファイル毎のセキュリティ情報（所有者ＩＤ、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）を予め登録したものである。このセキュリティ情報は、サーバ１の管理者が適宜登録する。

【００２５】以上のように、サーバ１が管理するファイルについて、ディレクトリ毎にセキュリティ情報、およびファイル毎にセキュリティ情報を付加してセキュリティを管理し、クライアント１１にダウンロードするときにファイルのデータにこのセキュリティ情報を付加して送信する。受信したクライアントではこのセキュリティ情報をファイル内のデータに付加しておく。

【００２６】次に、図４のフローチャートに示す順序に従い、図１ないし図３の構成のもとで、サーバ１からファイルをクライアント１１にダウンロードしてセキュリティ情報を当該ファイル書き込むときの手順を詳細に説明する。

【００２７】図４は、本発明のダウンロードフローチャート（セキュリティ情報の書き込み）を示す。図４にお

いて、Ｓ１は、サーバに接続し、ユーザ認証する。これは、クライアント１１が回線を介してサーバ１に接続し、ユーザＩＤ、パスワードを入力して送信し、サーバ１の資格チェック手段２がユーザ管理テーブル４を参照してユーザＩＤに対応づけてパスワードが登録され、資格があるか否かをチェックする。ＯＫのときにＳ２に進む。

【００２８】Ｓ２は、ファイル受信する。これは、Ｓ１で資格チェックしてＯＫとなったので、サーバ１がファイル３をダウンロードし、クライアント１１がファイルを受信する。

【００２９】Ｓ３は、セキュリティ情報を受信する。これは、Ｓ２でファイルをサーバ１がダウンロードしてクライアント１１が受信したことに続き、サーバ１がダウンロードしたファイルのアクセス権テーブル５を参照してセキュリティ情報として、

・所有者ＩＤ：Ａ
・グループ名：Ｘ
・グループに対するアクセス権：有／無
・その他に対するアクセス権：有／無
・その他

をダウンロードし、クライアント１１が受信する。ここで、セキュリティ情報は、図３のアクセス権テーブル５を参照し、ダウンロードしたファイルのディレクトリおよび当該ファイルのセキュリティ情報の両者を読み出し、より厳しい値（ＡＮＤ条件の値）を生成しセキュリティ情報としてクライアント１１にダウンロードし、セキュリティ管理の完備したサーバ１からセキュリティ管理の無いクランアント１１にこのセキュリティ情報を渡したこととなる。

【００３０】Ｓ４は、ファイル内にセキュリティ情報を書き込む。これは、クライアント１１がＳ２で受信したファイルに、Ｓ３で受信したセキュリティ情報を当該ファイルに書き込む。

【００３１】以上によって、セキュリティ管理の完備したサーバにおけるファイルのセキュリティ情報を、ダウンロードを受けたクライアント１１でファイル自身に当該セキュリティ情報を書き込み、セキュリティ管理する準備が完了したこととなる。

【００３２】図５は、本発明のダウンロードフローチャート（ドメイン名の書き込み）を示す。ここで事前にドメイン名を登録しておく。例えばクライアント１１を起動した管理者が画面上からドメイン名を入力して当該クラアイント１１のファイル１４にドメイン名、例えば“営業部”を登録する。これにより、以降は利用者は、同一のドメイン名のファイルしかアクセスできないようにロックされることとなる。

【００３３】図５において、Ｓ１１は、サーバに接続する。そして、既述した図４のＳ１と同様に資格チェックを受け、ＯＫのときにＳ１２に進む。Ｓ１２は、ファイル受信する。これは、クライアント１１がサーバ１からファイルを受信する。



【００３４】Ｓ１３は、クライアントがファイルを作成する。Ｓ１４は、ファイル内にドメイン名を書き込む。これは、Ｓ１２でサーバ１からダウンロードされて受信したファイル、あるいはＳ１３でクライアント内で作成したファイルについて、ドメイン名を書き込む。ドメイン名は、例えば後述する図９に示すように、このファイルのアクセスを許可するドメイン名、例えば“営業部”、“総務部”、“経理部”などをファイルに書き込み、当該ドメイン名が書き込まれたファイルについて、同一のドメイン名が予め登録されたクライアント（端末）１１しか当該ファイルをアクセスできないようにクライアント１１のアクセス権確認手段１３が制御する。

【００３５】以上によって、ダウンロードを受けたファイルあるいは作成したファイルに対してドメイン名を書き込み、当該ドメイン名の登録されたクライアント（端末）１１しか当該ファイルをアクセスできないようにアクセス権確認手段１３が制御を行うことが可能となる。

【００３６】図６は、本発明のダウンロードしたファイルに対するアクセスフローチャートを示す。図６において、Ｓ２２は、サーバに接続する。そして、ユーザ認証する。これは、クライアント１１が回線を介してサーバ１に接続し、ユーザＩＤ、パスワードを入力して送信し、サーバ１の資格チェック手段２がユーザ管理テーブル４を参照してユーザＩＤに対応づけてパスワードが登録され、資格があるか否かをチェックする。ＯＫのときにＳ２３に進む。

【００３７】Ｓ２３はユーザＩＤが所属しているグループ名を受信する。これは、既述した図２のユーザ管理テーブル４を参照し、ユーザＩＤが所属しているグループ名を取り出して受信する。

【００３８】Ｓ２４は、サーバとの接続を切断する。以上のＳ２１からＳ２４によって、クライアント（端末）１１に、サーバから当該ユーザＩＤのグループ名を受信する。

【００３９】Ｓ２５は、ファイルをアクセスする。これは、あるユーザＩＤの利用者がクライアント１１の保持するあるファイル１５をアクセスしようとする。Ｓ２６は、ドメイン名が一致か判別する。これは、Ｓ２５でアクセスしようとしたファイル１５に書き込まれているドメイン名と、当該クライアント（端末）１１に管理者が事前に登録したドメイン名とが一致するか判別する。ＹＥＳの場合には、Ｓ２７に進む。一方、ＮＯの場合には、ドメイン名が一致しなく当該ファイルへのアクセスが許可できないので、Ｓ３３でアクセス不可とし、Ｓ３４エラー処理を行い、終了する。

【００４０】Ｓ２７は、ユーサＩＤとフィイル内の所有者が一致か判別する。これは、Ｓ２５でアクセスしようとした利用者のユーザＩＤと、アクセスしようとしたフ

ァイル内に書き込まれている所有者ＩＤとが一致し、アクセス権がありか判別する。ＹＥＳの場合には、アクセス権有と判明したので、Ｓ３１でアクセス可と判定し、Ｓ３２でアクセスを行う。一方、Ｓ２７のＮＯの場合には、所有者でないと判明したので、Ｓ２８に進む。

【００４１】Ｓ２８は、グループ名とファイル内のグループ名が一致か判別する。これは、Ｓ２３で受信したユーザＩＤが所属するグループ名と、Ｓ２５でアクセスしようとしたファイル内に書き込まれているグループ名と一致か判別する。ＹＥＳの場合には、更に、Ｓ２９でファイル内に書き込まれているグループに対するアクセス権の有無を読み出し、有のときにＳ３１でアクセス可と判定しＳ３２でアクセスし、無のときにＳ３３でアクセス不可と判定しＳ３４でエラー処理し終了する。一方、Ｓ２８のＮＯの場合には、更にＳ３０でファイル内に書き込まれているその他に対するアクセス権の有無を読み出し、有のときにＳ３１でアクセス可と判定しＳ３２でアクセスし、無のときにＳ３３でアクセス不可と判定しＳ３４でエラー処理し終了する。

【００４２】以上によって、ファイル内に書き込まれているドメイン名、所有者名、グループ名、グループに対するアクセス権の有無、およびその他に対するアクセス権の有無に従い、アクセス権有りと判明したとき（Ｓ２７のＹＥＳ、Ｓ２８のＹＥＳかつＳ２９の有、Ｓ２８のＮＯかつＳ３０の有のいずれかのとき）に、ファイルのアクセスを許可し、セキュリティ機能のないクライアント（端末）１１であっても、本発明によってサーバ1が持つセキュリティ情報に従ったセキュリティ管理を行うことが可能となる。

【００４３】図７は、本発明のドメイン名登録フローチャートを示す。これは、既述した図５の事前にドメイン名登録の詳細手順である。図７において、Ｓ４１は、管理システムのインストールする。これは、図１のクライアント１１で管理システム（登録手段１２、アクセス権確認手段１３などの管理システム）をインストールする際に、ドメイン名およびアクセス権のセキュリティの有無について、いずれか一方、あるいは両者をチェックするかの区別を登録する。これにより、ドメイン名のみによるアクセス権のチェック、セキュリティ情報のみによるアクセス権のチェック、あるいは両者によるアクセス権のチェックのいずれかがインストール時などに設定されることとなる。

【００４４】Ｓ４２は、ドメイン名を入力する。Ｓ４３は、ドメイン名を登録する（図１のファイル１４を作成する）。これらＳ４２およびＳ４３は、管理者がクライアント（端末）１１に管理システムをインストールする際に、アクセス権のチェックする仕方（ドメイン名のみ、セキュリティ情報のみ、あるいは両者）を設定する。

【００４５】以上によって、クライアント（端末）１１のインストール時などに管理者がドメイン名、セキュリティ情報、あるいは両者によるアクセス権のチェックを行うかを任意に設定することが可能となる。

【００４６】図８は、本発明のファイルアクセスフローチャートを示す。これは、ドメイン名によってアクセス権をチェックするときの手順である。図８において、Ｓ５１は、ファイルのアクセスをしようとする。

【００４７】Ｓ５２は、ドメイン名とファイル内のドメイン名とが一致か判別する。これは、利用者が操作したクラインアト１１に登録されているドメイン名と、Ｓ５１でアクセスしようとしたファイルに書き込まれているドメイン名とが一致か判別する。ＹＥＳの場合には、一致してアクセス権有と判明したので、Ｓ５３でアクセス可と判定し、Ｓ５４でアクセスを行う。一方、ＮＯの場合には、一致しなくアクセス権無と判明したので、Ｓ５５でアクセス不可と判定し、Ｓ５６でエラー処理を行い、終了する。

【００４８】図９は、本発明のドメインの説明図を示す。ここで、ドメインは特定の部署が使用するクライアント（端末）１１に登録して当該ドメイン名が書き込まれてたファイルのアクセスのみを可能し、クライアント１１とファイルとをドメイン名でロックするようにしたものである。ここでは、図示のように

・ドメイン1として、営業部のクライアント（端末）１１を３台割り当て、既述した図７のフローチャートに従い、同一のドメイン名“ドメイン1”を当該クライアント１１に登録する。

【００４９】・ドメイン2として、総務部のクライアント（端末）１１を３台割り当て、既述した図７のフローチャートに従い、同一のドメイン名“ドメイン2”を当該クライアント１１に登録する。

【００５０】・ドメイン3として、経理部のクライアント（端末）１１を３台割り当て、既述した図７のフローチャートに従い、同一のドメイン名“ドメイン3”を当該クライアント１１に登録する。

【００５１】以上のように、ドメイン名“ドメイン1”、“ドメイン2”、“ドメイン3”をそれぞれ営業部、総務部、経理部が利用するクライアント（端末）１１に図７のフローチャートに従い登録することにより、これら各クライアント（端末）１１は、媒体中のファイルのうち、各自のドメイン名が一致するファイルのみをアクセスすることが可能となり、他のクライアント１１はアクセスできず、セキュリティを確保することが可能となる。

【００５２】

【発明の効果】以上説明したように、本発明によれば、セキュリティ機構を持たない情報処理装置であっても、ファイル毎に所有者ＩＤ、グループ名、グループの権限の有無などのセキュリティ情報およびドメイン名を書き込んでおき、アクセス権確認手段１３がこれらをもとに

9

アクセス権の有無をチェックする構成を採用しているため、ファイル毎にセキュリティを管理することができる。これらにより、セキュリティ機構を持たないクライアント（端末）であっても、ファイルにセキュリティ情報およびドメイン名を書き込んでおき、媒体などに格納されたファイルのセキュリティを簡易に管理することが可能となる。

【図面の簡単な説明】

【図１】本発明のシステムブロック図である。

【図２】本発明のユーザ管理テーブル例である。

【図３】本発明のアクセス権テーブル例である。

【図４】本発明のダウンロードフローチャート（セキュリティ情報の書き込み）である。

【図５】本発明のダウンロードフローチャート（ドメイン名の書き込み）である。

【図６】本発明のダウンロードしたファイルに対するアクセスフローチャートである。

10

＊【図７】本発明のドメイン名登録フローチャートである。

【図８】本発明のファイルアクセスフローチャートである。

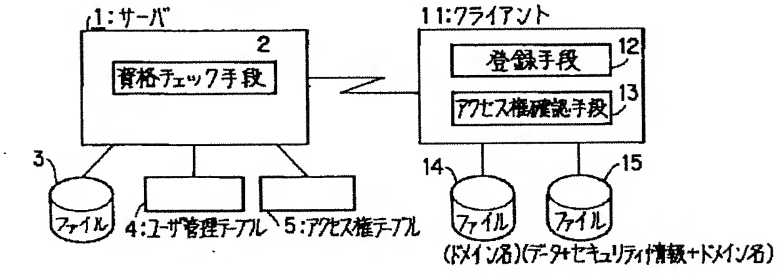
【図９】本発明のドメインの説明図である。

【符号の説明】

１：サーバ
２：資格チェック手段
３：ファイル
４：ユーザ管理テーブル
５：アクセス権テーブル
１１：クライアント（端末）
１２：登録手段
１３：アクセス権確認手段
１４：ファイル（ドメイン名）
１５：ファイル（データ＋セキュリティ情報＋ドメイン名）

【図１】

本発明のシステムブロック図




【図２】

本発明のユーザ管理テーブル例

4

| ユーザID | パスワード | グループ名 |
|---|---|---|
| U01 | 011 | X |
| ⋮ | ⋮ | ⋮ |

【図３】

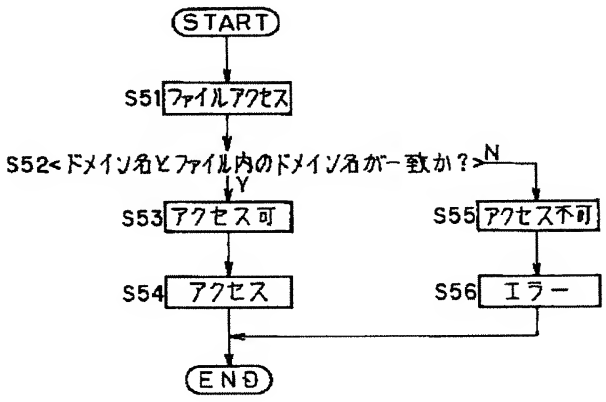
本発明のアクセス権テーブル例

5

| ディレクトリXX<br>・所有者<br>・グループ：有／無<br>・その他：有／無 | ファイルXXX | :所有者<br>:グループ:有／無<br>:その他 :有／無 |
|---|---|---|
| | ⋮ | |
| | ⋮ | |
| | ⋮ | |

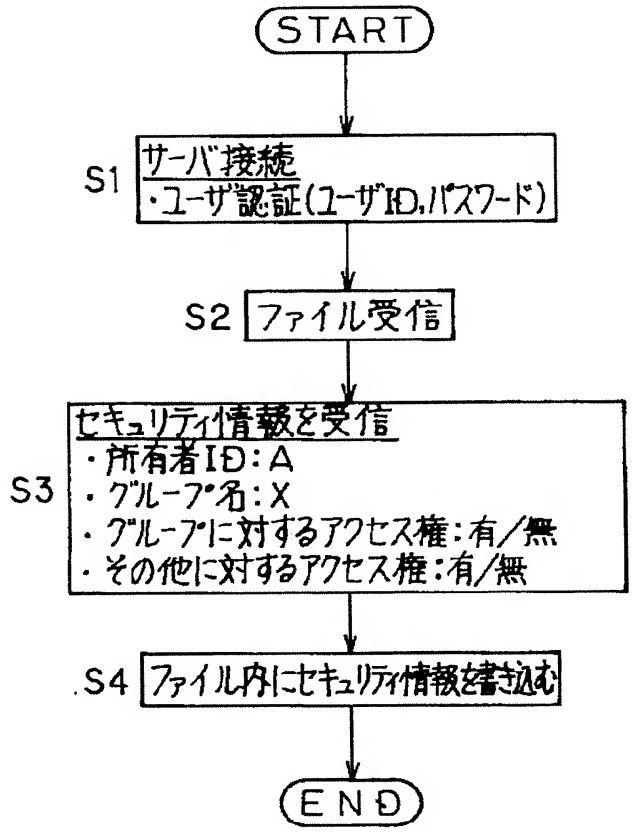
【図８】

本発明のファイルアクセスフローチャート



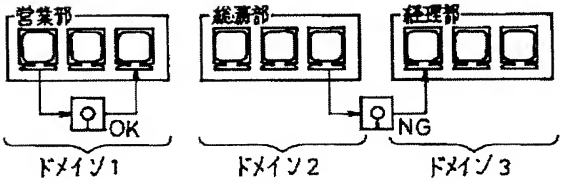
【図４】

本発明のダウンロードフローチャート（セキュリティ情報の書き込み）



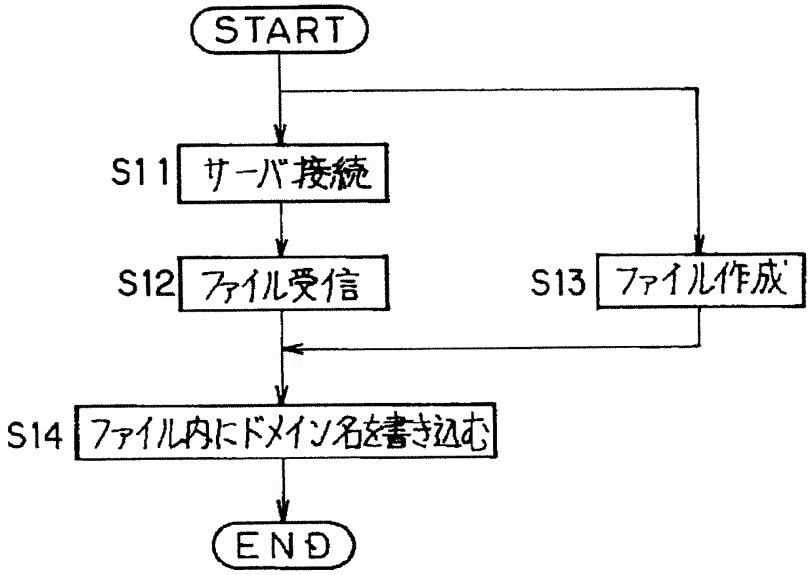

【図９】

本発明のドメインの説明図



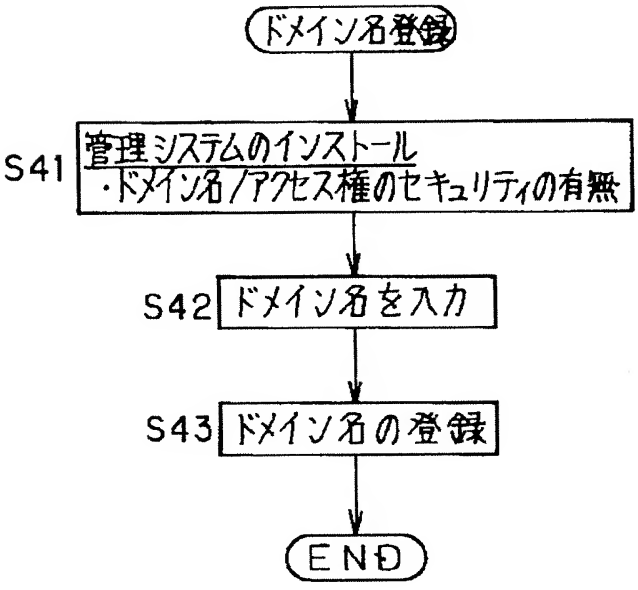
【図５】

本発明のダウンロードフローチャート（ドメイン名の書き込み）




【図７】

本発明のドメイン名登録フローチャート



【図６】

本発明のダウンロードしたファイルに対するアクセスフローチャート